AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in this patent application.

Listing of Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

Claim 1 (Currently Amended): A ~~computer~~ system implemented on a computer apparatus for processing a computer file to determine whether it contains a virus or other malware comprising:

a) means for generating data with regard to the file to characterise its identity and for thereby referencing a computer database to determine whether it is an instance of a known file;

b) means for selectively subjecting the file to a number of heuristic procedures to determine whether or not it contains, or is likely to contain, malware; and

c) means for determining, in dependence upon the record, if any, of the file in the database, whether the file can be regarded as safe in dependence on factors including a factor that the longer the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected the more likely that the file is safe and for controlling the means b) such that the file, if the file is to be regarded as safe, is either subject to less thorough processing than if it were not so regarded or not subject to processing by the means b) at all.

Claim 2 (Canceled).

Claim 3 (Currently Amended): A ~~computer~~ system according to claim 1 wherein the means c) performs said determining of whether the file can be regarded as safe in dependence on factors including sources, recorded in the database, from which instances of the file have originated.

Claim 4 (Currently Amended): A ~~computer~~ system according to claim 1 wherein the means c) performs said determining of whether the file can be regarded as safe in dependence on factors including the number of times, recorded in the database, instances of the file have been processed.

Claim 5 (Currently Amended): A ~~computer~~ system according to claim 1 and including means for updating the database in dependence upon the result of the processing of the file by the means b).

Claim 6 (Currently Amended): A ~~computer~~ system according to claim 5 wherein the means for updating the database, is operative in the event of the means b) determining that the file contains, or is likely to contain, malware to delete the record of the file in the database, or to update the record of the file in the database so that the file is no longer taken be safe.

Claim 7 (Currently Amended): A method of processing a computer file to determine whether it contains a virus or other malware comprising:

a) generating data with regard to the file to characterise its identity and for thereby referencing a computer database to determine whether it is an instance of a known file;

b) selectively subjecting the file to a number of heuristic procedures to determine whether or not it contains, or is likely to contain, malware;

c) determining, in dependence upon the record, if any, of the file in the database, whether the file can be regarded as safe in dependence on factors including a factor that the longer the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected the more likely that the file is safe and conducting the step b) such that the file, if the file is to be regarded as safe, is either subject to less thorough processing than if it were not so regarded or not subject to processing by the step b) at all; and

d) storing the determination of whether or not the file contains, or is likely to contain, malware.

Claim 8 (Canceled).

Claim 9 (Previously Presented): A method according to claim 7 wherein the step c) of determining whether the file can be regarded as safe is performed in dependence on factors including sources, recorded in the database, from which instances of the file have originated.

Claim 10 (Previously Presented) A method according to claim 7 wherein the step c) of determining whether the file can be regarded as safe is performed in dependence on factors including the number of times, recorded in the database, instances of the file have been processed.

Claim 11 (Previously Presented): A method according to claim 7 and including the step of updating the database in dependence upon the result of the processing of the file by the step b).

Claim 12 (Previously Presented): A method according to claim 11 wherein the updating of the database comprises, in the event of the step b) determining that the file contains, or is likely to contain, malware, deleting the record of the file in the database, or updating the record of the file in the database so that the file is no longer taken be safe.

Claim 13 (Currently Amended): A ~~computer~~ system implemented on a computer apparatus for processing a computer file to determine whether it contains a virus or other malware, ~~and~~ the system comprising an engine that generates data with regard to the file to characterise its identity and for thereby referencing a computer database to determine whether it is an instance of a known file; that processes the file by selectively subjecting the file to a number of heuristic procedures to determine whether or not it contains, or is likely to contain, malware; that determines, in dependence upon the record, if any, of the file in the database, whether the file can be regarded as safe in dependence on factors including a factor that the longer the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected the more likely that the file is safe; and ~~for controlling~~ that controls the processing to which the file is subjected such that the file, if the file

is to be regarded as safe, is either subject to less thorough processing than if it were not so regarded or not subject to the processing at all.